Amendments to the Claims

This listing of claims will replace all prior versions, and listings, of claims in the application:

Listing of Claims:

1-10. (Cancelled)

11. (New) A cryptographic method employed between two entities exchanging information via a non-secure communication channel, each of the two entities comprising a memory readable by a machine, tangibly embodying a program of instruction executable by the machine to perform the method, the method including a step of multiplying an odd order point of a non-supersingular elliptic curve by an integer, wherein, for exchanging information via the non-secure communication channel, the step of addition and halving of points of said elliptic curve, the halving of a point P is defined as a unique odd order point D such that [2]D = P, $\left[\frac{1}{2}\right]$ denotes the halving operation and $\left[\frac{1}{2}\right]$P denotes the point D.

12. (New) A method according to claim 11, where F_{2^n} is a finite body of 2^n elements, $E(F_{2^n})$ is the sub-group of an elliptic curve E defined by:

$$E(F_2^n) = \{(x,y) \in F_2^n \times F_2^n \mid y^2 + xy = x^3 + \alpha x^2 + \beta\} \cup \{0\} \quad \alpha, \beta \in F_2^n, \beta \neq 0$$

and $E[2^k]$ is the set of points P of said elliptic curve such that P added 2^k times to itself gives the neutral element *O*, where k is an integer greater than or equal to 1, wherein a point $P = (x,y)$ of said elliptic curve gives by said halving the point $\left[\frac{1}{2}\right]P = (u_o, v_o)$ of said elliptic curve obtained by effecting the following operations:

(a) seek a first value λ_o such that $\lambda_o^2 + \lambda_o = \alpha + x$;

(b) calculate a second value u_o^2 such that $u_o^2 = x\ (\lambda_o + 1) + y$;

(c) if k has the value 1, check if the equation: $\lambda^2 + \lambda = \alpha^2 + u^2_o$ has solutions in F_2^n;

(d) if the check in step (c) is yes, calculate said halving as follows:

$$u_o = \sqrt{u_0^{\,2}}\ ,$$

$$v_o = u_o\ (u_o + \lambda_o)\ ,$$

and $\left[\frac{1}{2}\right]\ P = (u_o,\ v_o)$;

(e) if not, add x to said second value u_o^2 and 1 to said first value λ_o and calculate said halving as in step (d);

(f) if k is greater than 1, perform an iterative calculation as follows:

(i) seek a value λ_i such that $\lambda_i^2 + \lambda_i = \alpha + u_{i-1}$; and

(ii) then calculate the value u^2_i such that $u^2_i = u_{i-1}\ (\lambda_i + \lambda_{i-1} + u_{i-1} + 1)$ by incrementing i from i=1 until the value u^2_{k-1} is obtained;

(g) check whether the equation $\lambda^2 + \lambda = \alpha^2 + u^2_{k-1}$ has solutions in F_2^n ;

(h) if so, calculate said halving as follows:

$$u_o = \sqrt{u_0^{\,2}}\ ,$$

$$v_o = u_o\ (u_o + \lambda_o)\ ,$$

and $\left[\frac{1}{2}\right] P = (u_o,\ v_o)$; and

(i) if not, add x to the second value u_o^2 and 1 to said first value λ_o and calculate said halving as in step (h).

13. (New) A method according to claim 11, where F_2^n is a finite body of 2^n elements, $E(F_2^n)$ is the sub-group of an elliptic curve E defined by:

$$E(F_2^n) = \{(x,y) \in F_2^n \times F_2^n \mid y^2 + xy = x^3 + \alpha x^2 + \beta\} \cup \{O\}\ \alpha,\ \beta \in F_2^n,\ \beta \neq 0$$

and $E[2^k]$ is the set of points P of said elliptic curve such that P added 2^k times to itself gives the neutral element O, where k is an integer greater than or equal to 1, wherein a point P = (x,y) of said elliptic curve gives by said halving the point $\left[\frac{1}{2}\right]P = (u_o,\ \lambda_o)$ of said elliptic curve,

with $\lambda_o = u_o + v_o/u_o$, obtained by effecting the following operations:

(a) seek a first value λ_o such that $\lambda_o^2 + \lambda_o = \alpha + x$;

(b) calculate a second value u_o^2 such that : $u_o^2 = x(\lambda_o + 1) + y$;

(c) if k has the value 1, check if the equation : $\lambda^2 + \lambda = \alpha^2 + u_o^2$ has solutions in F_{2^n};

(d) if so, calculate said halving as follows :

$u_o = \sqrt{u_0^2}$,

and $\left[\frac{1}{2}\right]P = (u_o, \lambda_o)$;

(e) if not, add x to said second value u_o^2 and 1 to said first value λ_o and calculate said halving as in step (d);

(f) if k is greater than 1, perform the following iterative calculation:

(i) seek a value λ_i, such that $\lambda_i^2 + \lambda_i = \alpha + u_{i-1}$; and

(ii) then calculate the value u_i^2 such that $u_i^2 = u_{i-1}(\lambda_i + \lambda_{i-1} + u_{i-1} + 1)$ by incrementing i from i = 1 until the value u^2_{k-1} is obtained;

(g) check if the equation $\lambda^2 + \lambda = \alpha^2 + u^2_{k-1}$ has solutions in F_{2^n};

(h) if so, calculate said halving as follows:

$u_o = \sqrt{u_0^2}$, and

$\left[\frac{1}{2}\right]P = (u_o, \lambda_o)$; and

(i) if not, add x to said second value u_o^2 and 1 to said first value λ_o to calculate said halving as in step (h).

14. (New) A method according to claim 11, where F_2^n is a finite body of 2^n elements, $E(F_2^n)$ is the sub-group of an elliptic curve E defined by:

$E(F_2^n) = \{(x,y) \in F_2^n \times F_2^n \mid y^2 + xy = x^3 + \alpha x^2 + \beta\} \cup \{O\}$ $\alpha, \beta \in F_2^n$, $\beta \neq 0$ and $E[2^k]$ is the set of points P of said elliptic curve such that P added 2^k times to itself gives the neutral element O, where k is an integer greater than or equal to 1, wherein a point P = (x,y) of said elliptic curve represented by (x,λ_p) with $\lambda_p = x + y/x$ gives by said halving the point $\left[\frac{1}{2}\right]P = (u_o, v_o)$ of said elliptic curve obtained by effecting the following operations:

(a) seek a first value λ_o such that $\lambda_o^2 + \lambda_o = \alpha + x$;

(b) calculate a second value u_o^2 such that $u_o^2 = x(\lambda_o + \lambda_p + x + 1)$;

(c) if k has the value 1, check if the equation: $\lambda^2 + \lambda = \alpha^2 + u_o^2$ has solutions in F_2^n;

(d) if so, calculate said halving as follows:

$u_o = \sqrt{u_0^2}$,

$v_o = u_o\ (u_o + \lambda_o)$,

and $\left[\frac{1}{2}\right]P = (u_o,\ v_o)$;

(e) if not, add x to said second value u_o^2 and 1 to said first value λ_o and calculate said halving as in step (d);

(f) if k is greater than 1, perform the following iterative calculation:

(i) seek a value λ_i such that $\lambda_i^2 + \lambda_i = \alpha + u_{i-1}$; and

(ii) then calculate the value u_i^2 such that $u_i^2 = u_{i-1}\ (\lambda_i + \lambda_{i-1} + u_{i-1} + 1)$ incrementing i from i=1 until the value u^2_{k-1} is obtained;

(g) check if the equation $\lambda^2 + \lambda = \alpha^2 + u^2_{k-1}$ has solutions in F_2^n;

(h) if so, calculate said halving as follows:

$u_o = \sqrt{u_0^2}$,

$v_o = u_o\ (u_o + \lambda_o)$,

and $\left[\frac{1}{2}\right]P = (u_o,\ v_o)$; and

(i) if not, add x to said second value u_o^2 and 1 to said first value λ_o and calculate said halving as in step (h).

15. (New) A method according to claim 11, where F_2^n is a finite body of 2^n elements, $E(F_2^n)$ is the sub-group of an elliptic curve E defined by:

$E(F_2^n) = \{(x,y) \in F_2^n \times F_2^n \mid y^2 + xy = x^3 + \alpha x^2 + \beta\} \cup \{O\}$ $\alpha, \beta \in F_2^n$, $\beta \neq 0$ and $E[2^k]$ is the set of points P of said elliptic curve such that P added 2^k times to itself gives the neutral element O, where k is an integer greater than or equal to 1, wherein a point $P = (x,y)$ of said elliptic curve represented by (x,λ_p) with $\lambda_p = x + y/x$ gives by said halving the point $\left[\frac{1}{2}\right]P = (u_o, v_o)$ of said elliptic curve represented by (u_o, λ_o), with $\lambda_o = u_o + v_o/u_o$ obtained by effecting the following operations:

(a) seek for a first value λ_o such that $\lambda_o^2 + \lambda_o = \alpha + x$;

(b) calculate a second value u_o^2 such that $u_o^2 = x(\lambda_o + \lambda_p + x + 1)$;

(c) if k has the value 1, check if the equation $\lambda^2 + \lambda = \alpha^2 + u_o^2$ has solutions in F_2^n;

(d) if so, calculate said halving as follows:

$$u_o = \sqrt{u_0^2},$$

and $\left[\frac{1}{2}\right]P = (u_o, \lambda_o)$;

(e) if not, add x to said second value u_o^2 and 1 to said first value λ_o and calculate said halving as in step (d);

(f) if k is greater than 1, perform the following iterative calculation:

(i) seek a value λ_i such that $\lambda_i^2 + \lambda_i = \alpha + u_{i-1}$; and

(ii) then calculate the value u_i^2 such that $u_i^2 = u_{i-1}(\lambda_i + \lambda_{i-1} + u_{i-1} + 1)$ incrementing i from i=1 until the value u^2_{k-1} is obtained;

(g) check if the equation $\lambda^2 + \lambda = \alpha^2 + u^2_{k-1}$ has solutions in F_2^n;

(h) if so, calculate said halving as follows:

$$u_o = \sqrt{u_0^2},$$

and $\left[\frac{1}{2}\right]P = (u_o, \lambda_o)$; and

(i) if not, add x to said second value u_o^2 and 1 to said first value λ_o and calculate said halving as in step (h).

16. (New) A method according to claim 11, further comprising constructing a common key from two secret keys respectively belonging to the aforementioned two entities and a public key consisting of the point P of odd order r of a chosen non-supersingular elliptic curve E.

17. (New) A method according to claim 16, wherein a and b are the secret keys of first and second entities, respectively, and:

(a) the first entity calculates the scalar multiplication [a]P and sends the result point to the second entity,

(b) the second entity calculates the scalar multiplication [b]P and sends the result point to the first entity,

(c) the two entities respectively calculate a common point (C) = (x,y) of said elliptic curve (E) by respectively effecting the scalar multiplications [a] ([b]P) and [b] ([a]P), both equal to [a.b]P, and

(d) the two entities choose as their common key the coordinate (x) of said common point (C) obtained by said scalar multiplication [a.b]P, at least one of the preceding scalar multiplications, and preferably all of them, being effected by means of predefined halvings.

18. (New) A method according to claim 11, further comprising calculating a signature between two entities based on a pair of permanent keys belonging to one of the entities, one secret (a) and the other public (Q), by scalar multiplication of the secret key (a) by another public key

consisting of the point (P) of odd order r of a chosen non-supersingular elliptic curve (E).

19. (New) A method according to claim 18, further comprising the following operations:

(a) the first entity (A) holding said pair of permanent keys constructs a single-use pair of keys, one key (g) being chosen arbitrarily and the other key [g]P resulting from scalar multiplication of said arbitrarily chosen key (g) by the public point P of said elliptic curve, the coordinates of the key ([g]P) being denoted (x,y) with $2 \leq g \leq r-2$,

(b) the first entity (A) converts the polynomial x of said single-use key [g]P = (x,y) into an integer i whose binary value is represented by the sequence of binary coefficients of said polynomial x,

(c) said first entity (A) calculates a signature (c,d) of the message (M) as follows:

$c = i \text{ modulo } r$

$d = g^{-1} (M + ac) \text{ modulo } r$,

(d) said first entity sends said message (M) and said signature (c, d) to said second entity; upon receiving it:

(i) said second entity (B) checks if the elements of said signature (c,d) each belong to the range [1, r-1],

(ii) if the check in step (i) is no, the second entity declares the signature invalid and stops;

(iii) if the check in step (i) is yes, said second entity (B) calculates three parameters:

$h = d^{-1}$ modulo r,

$h_1 = Mh$ modulo r, and

$h_2 = ch$ modulo r,

(e) said second entity calculates a point T of said elliptic curve by summing the scalar multiplications of the points P and Q by the last two parameters cited:

$T = [h_1] P + [h_2] Q$, and

(i) if the resultant point T is the neutral element, said second entity declares the signature invalid and stops;

(ii) if the resultant point T is not the neutral element, considering the point T with coordinates x' and y': T = (x',y'),

(A) said second entity (B) converts the polynomial x' of that point into an integer i' whose binary value is represented by the sequence of binary coefficients or said polynomial x',

(B) said second entity (B) calculates c' = i' modulo r and,

(C) said second entity (B) checks if c' = c, in which case said second entity (B) validates said signature, or if not, said second entity (B) invalidates said signature, at least one aforementioned scalar multiplication operation being effected by means of the predefined halvings.

20. (New) A method according to claim 17, wherein scalar multiplication using halvings is obtained by the following operations:

(e) if said scalar of the multiplication is denoted S, choose m+1 values So... Sm $\in \{0,1\}$ to define S as follows:

$$S = \sum_{i=0}^{m} S_i \left(\frac{r+1}{2} \right)^i ,$$

r being the aforementioned odd order and m being the single integer between $\log_2(r) - 1$ and $\log_2(r)$,

(f) calculate the scalar multiplication [S]P of a point P of said elliptic curve by the scalar S by applying an algorithm consisting of determining the series of points (Q_{m+1}, Q_m..., Q_i..., Q_o) of said elliptic curve E such that:

Q_{m+1} = O (neutral element), and

$$Q_i = [S_i]P + \left[\frac{1}{2}\right] Q_{i+1} \text{ with } o \leq i \leq m, \text{ and}$$

(g) calculate the last point Q_o of said series giving the result [S]P of said scalar multiplication.

21. (New) A method according to claim 11, wherein said integer is decomposed as a set of values using powers of half said order, and said addition and halving operations are implemented dependent on said set of values.